ICS 35.040
L 80
备案号：62698-2019

DB11

北　京　市　地　方　标　准

DB11/T 1654—2019

信息安全技术 网络安全事件应急处置规范

Information security technology
Network security incidents emergency disposal regulations

2019 - 09 - 26 发布　　2020 - 01 - 01 实施

北京市市场监督管理局　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009提出的规则起草编写。

本标准由北京市公安局提出并归口。

本标准由北京市公安局组织实施。

本标准主要起草单位：北京市公安局、北京市委网信办、公安部第一研究所、中科信息安全共性技术国家工程研究中心有限公司。

本规范主要起草人：纪小默、赵悦、石锐、赵志巍、柳亮、尹航、王京军、张越今、问闻、李梦姣、周堃、菅强、张昕、宋扬、金镁、张红、石浩、俞诗源、杨虎、王海珍、万鹏。

信息安全技术 网络安全事件应急处置规范

1 范围

本标准规定了网络安全事件的网络安全事件分类与分级、调查处置、日常监测和应急工作准备。

本标准适用于非涉及国家秘密的信息系统运营使用者、行业主管部门、监管部门以及网络安全事件应急支撑队伍使用。

本标准不适用于涉及国家秘密的信息系统的安全事件调查处置。

2 术语和定义

下列术语和定义适用于本规范。

2.1

信息系统 information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2.2

网络安全事件 Network security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。如计算机病毒、特洛伊木马、拒绝服务攻击、漏洞攻击事件、网络扫描窃听攻击等事件。

2.3

应急处置 emergency disposal

通过采取断网或者停止服务等手段控制事态发展，防止事件蔓延。

2.4

信息安全等级保护 classified protection of information system security

指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的网络安全事件分等级响应、处置。下文所述的系统级别均为信息安全等级保护级别。

3 网络安全事件分类与分级

3.1 事件分类

3.1.1 安全风险

指因信息系统存在缺陷和风险，系统面临发生安全事故的事件。信息安全风险可以分为安全管理制度的制定或执行上存在的缺陷；系统在设计和建设时遗留下来的安全风险；系统硬件设施存在安全风险，说明如下：

a) 安全管理制度的制定或执行上存在的缺陷。如未定期进行应急演练或未定期更新完善应急预案等情况造成的安全风险；
b) 系统在设计和建设时遗留下来的安全风险。如带宽设计不足、系统存在漏洞等方面带来的安全风险；
c) 系统硬件设施存在安全风险，如部件老化或自带有可被攻击利用的功能模块等各种形式的硬件设施安全风险。

3.1.2 安全攻击事件

指通过网络或其他技术手段，利用信息系统的缺陷或使用暴力攻击对信息系统实施攻击，或人为使用非技术手段对信息系统进行破坏，而造成信息系统异常的事件。安全攻击事件可以分为有害程序事件、网络攻击事件、信息破坏事件和物理破坏事件等，说明如下：

a) 有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；
b) 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；
c) 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；
d) 物理破坏事件是指蓄意地对保障信息系统正常运行的硬件、软件等实施 窃取、破坏造成的网络安全事件。

3.1.3 设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的网络安全事件，以及人为的使用非技术手段无意的造成信息系统设备设施损坏的网络安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障和其它设备设施故障等3个子类，说明如下：

a) 软硬件自身故障：是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的网络安全事件；
b) 外围保障设施故障：是指由于保障信息系统正常运行所必须的外部设施自身出现故障而导致的网络安全事件，例如电力故障、外围网络故障等导致的网络安全事件；
c) 其它设备设施故障：是指不能被包含在以上 2 个子类之中的设备设施故障而导致的网络安全事件。

3.1.4 灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的网络安全事件。 灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的网络安全事件。

3.1.5 其他

不属于以上四类的网络与网络安全事件。

3.2 事件分级

3.2.1 Ⅰ级

符合下列情形之一的，为Ⅰ级网络与网络安全事件：

a) 等级保护3级（含）以上信息系统，发生系统中断运行或出现严重信息泄露，造成严重影响。
b) 等级保护3级（含）以上信息系统，发生数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁，或导致严重经济损失。
c) 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络与网络安全事件。

3.2.2 Ⅱ级

符合下列情形之一且未达到Ⅰ级的，为Ⅱ级网络与网络安全事件：

a) 等级保护2级信息系统，发生系统中断运行或出现严重泄露，造成较严重影响。
b) 等级保护2级信息系统，发生数据丢失或被窃取、篡改、假冒，对国家安全和社稳定构成威胁，或导致较严重经济损失。
c) 其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络与网络安全事件。

3.2.3 Ⅲ级

除上述情形外的其它网络与网络安全事件为一般事件。

4 网络安全事件调查处置

4.1 事件发现及处置

4.1.1 分级处置

4.1.1.1 Ⅰ级网络安全事件处置

发生Ⅰ级网络安全事件后，事发单位、监管部门、行业主管、技术支持单位、公安机关应按照图1所示的Ⅰ级网络安全事件处置流程分别开展工作。

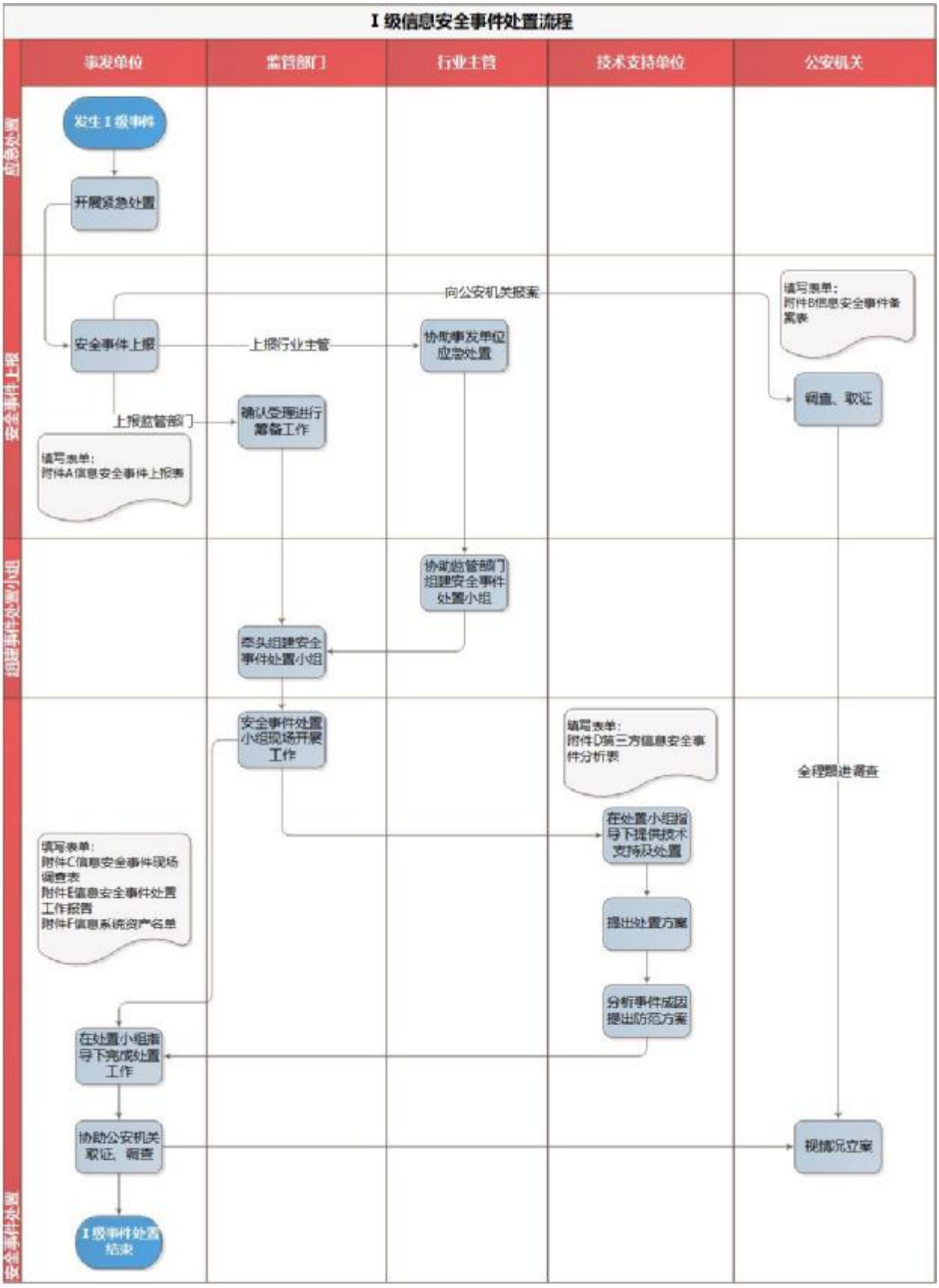

图 1 Ⅰ级网络安全事件处置流程

4.1.1.1.1 网络安全事件处置

由于Ⅰ级事件对应信息系统等级较高，涉及范围更广，网络安全事件处置小组需确保足够的资源及技术能力，以应对可能存在的各项工作，包括值班、出差、技术分析、系统加固、系统验证等方面的工作。

a) 事发单位首先开展应急处置工作，同时填报《网络安全事件上报表》(见附录A中表A.1)，将安全事件上报监管部门、行业主管并向公安机关报案。
b) 监管部门收到Ⅰ级安全事件报告后，牵头组建网络安全事件处置小组，由监管部门、公安机关、行业主管、事发单位以及技术支持单位等共同组成。由监管部门统一指挥安全事件处置；
c) 行业主管负责协助监管部门组建处置小组并指导事发单位开展事件紧急处置工作；
d) 事发单位负责在处置小组的指导下开展处置工作的实施，协助公安机关取证、调查，并填报《第三方网络安全事件分析表》（见附录B中表B.1）；
e) 技术支持单位负责在处置小组指导下提供技术支持，提出处置方案，并分析事件成因，提出防范方案；
f) 公安机关负责取证、调查以及立案的工作，并填写《网络安全事件备案表》（见附录C中表C.1）。

4.1.1.1.2 判断网络安全事件类型并进行应急处置

被攻击信息系统具备完善的应急处理机制的，信息系统运营使用者可结合网络安全事件具体情况，依据信息系统运营使用者及其行业主管部门制定的信息安全应急响应措施、策略及流程，开展应急处置工作，并填报《网络安全事件现场调查表》(附录D中表D.1）Ⅰ级事件对应的信息系统均符合等级保护三级以上要求，具备如双机双线、异地存储等措施，可以快速恢复系统功能，但过程中要注意保存相关证据，便于公安机关立案调查。

被攻击信息系统的应急处理机制缺失的，可参考以下内容进行应急处置，并填报《网络安全事件现场调查表》，具体要求如下：

a) 发生安全攻击类事件时，如果确认重要数据被窃取且事件还在持续发生，在确定被窃取系统的范围后，将被破坏系统和正常的系统进行隔离，断开或暂时关闭被破坏系统，必要时应立即切断网络，防止数据进一步损失，保护数据安全；
b) 发生安全攻击类事件时，如果信息系统被持续攻击，造成系统无法正常运行。须通过技术手段持续监测系统及网络状态，记录异常流量的远程IP、域名和端口，分析原因。事件处置人员须及时保护现场，配合公安机关现场调查与取证；
c) 发生信息内容安全类事件时，信息系统被篡改、假冒,造成严重社会影响。信息系统运营使用者须完整保存被篡改的网站系统，避免重要线索数据丢失。然后，采取技术手段立即删除恶意信息，停止信息的传播。事件处置人员须保存数据信息、保存日志、源代码等文件，用于技术分析及取证调查；
d) 发生设备设施故障类安全事件时，基础设施被破坏导致网络链路断开、设备损坏、电力故障、物品丢失被盗等事件。须立即启用备用设备、冗余链路、冗余电力。同时，保存门禁系统出入记录、视频监控信息，在系统恢复后通过该记录信息查找可疑人员。

4.1.1.1.3 制定处置方案并实施

安全事件得到控制后，网络安全事件处置小组充分评估被破坏系统的影响范围、影响程度，上报有关部门，通报有关单位，做好沟通协调工作。同时，调动一切资源及时设计处置方案。网络安全事件处

置小组须组织专家团队，对方案进行论证与评审后，方可实施。如果实施工作涉及第三方单位，须签署合同、授权书及人员保密协调，以确保实施内容及质量可控。

4.1.1.2 II级网络安全事件处置

发生II级网络安全事件后，事发单位、监管部门、行业主管、技术支持单位、公安机关应按照图2所示的II级网络安全事件处置流程分别开展工作。

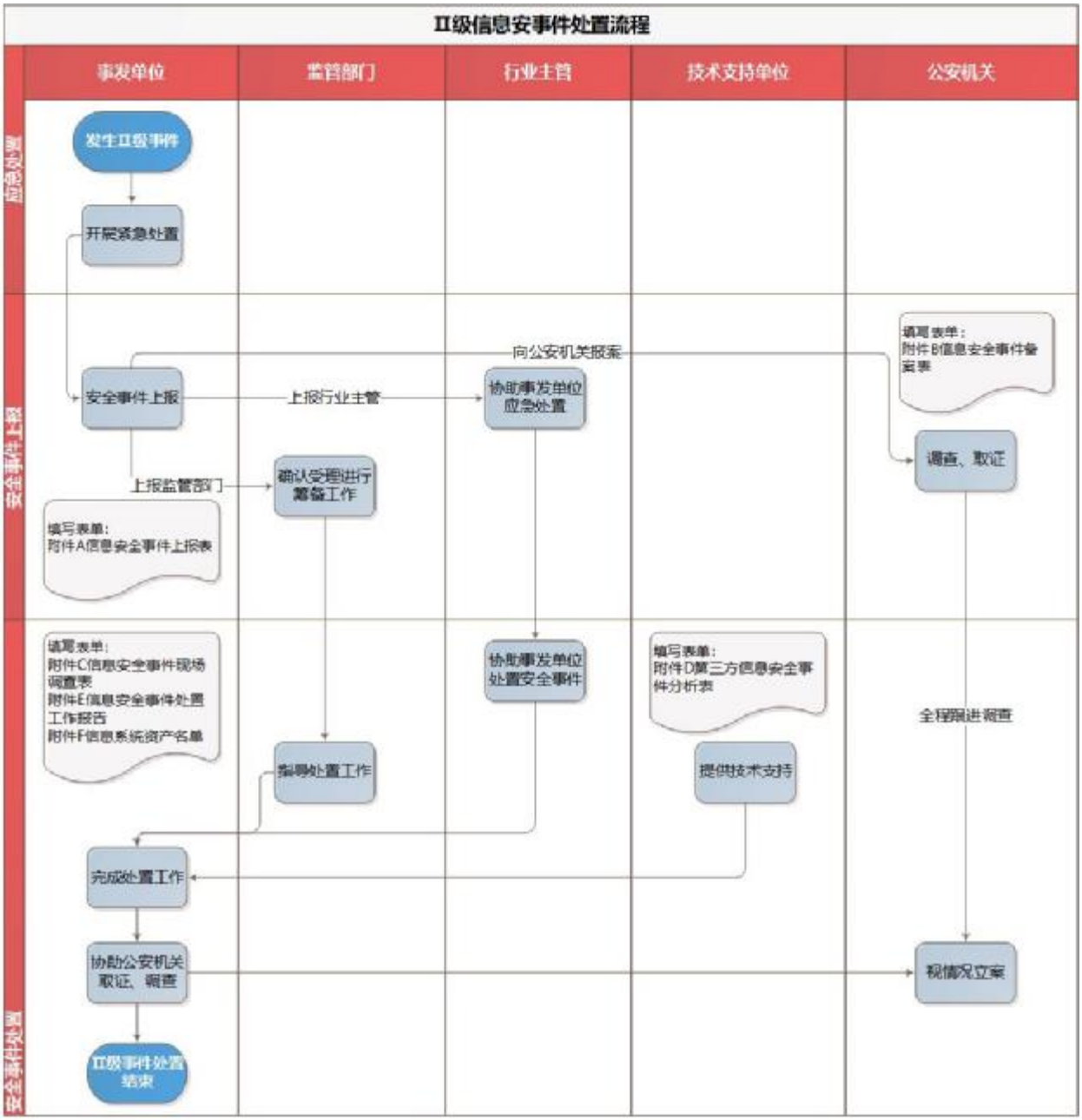

图 2 II级网络安全事件处置流程

4.1.1.2.1 网络安全事件处置

发生II级网络安全事件后，开展以下工作：

a) 事发单位立即开展应急处置工作，同时，上报监管部门、行业主管并向公安机关报案；
b) 监管部门根据实际情况指导指导事发单位进行事件的处置工作；
c) 行业主管应协助事发单位共同开展安全事件的处置工作；
d) 事发单位应积极协助公安机关进行立案、取证、调查等工作；
e) 技术支持单位负责技术支持工作；
f) 公安机关负责取证、调查以及立案的工作。

4.1.1.2.2 判断网络安全事件类型并进行应急处置

被攻击信息系统具备完善的应急处理机制的，信息系统运营使用者可结合网络安全事件具体情况，依据信息系统运营使用者及其行业主管部门制定的信息安全应急响应措施、策略及流程，开展应急处置工作，并填报《网络安全事件现场调查表》。过程中要注意保存相关证据，便于公安机关立案调查。具体要求如下：

a) 发生安全攻击类事件时，如果确认重要数据被窃取且事件还在持续发生，在确定被窃取系统的范围后，将被破坏系统和正常的系统进行隔离，断开或暂时关闭被破坏系统，必要时应立即切断网络，防止数据进一步损失，保护数据安全；
b) 发生安全攻击类事件时，如果信息系统被持续攻击，造成系统无法正常运行。须通过技术手段持续监测系统及网络状态，记录异常流量的远程 IP、域名和端口，分析原因。事件处置人员须及时保护现场，配合公安机关现场调查和取证；
c) 发生信息内容安全类事件时，信息系统被篡改、假冒,（如:国家机关门户网站被篡改）造成严重社会影响。信息系统运营使用者须采取技术手段立即删除恶意信息，停止信息的传播。事件处置人员须保存数据信息、保存日志、源代码等文件，用于技术分析及取证调查；
d) 发生设备设施故障类安全事件时，基础设施被破坏导致网络链路断开、设备损坏、电力故障、物品丢失被盗等事件。须立即启用备用设备、冗余链路、冗余电力。同时，保存门禁系统出入记录、视频监控信息，在系统恢复后通过该记录信息查找可疑人员。

4.1.1.2.3 制定处置方案并实施

安全事件得到控制后，网络安全事件处置小组充分评估被破坏系统的影响范围、影响程度，上报有关部门，通报有关单位，做好沟通协调工作。同时，进行处置方案设计并实施。如果实施工作涉及第三方单位，须签署合同、授权书及人员保密协调，以确保实施内容及质量可控。

4.1.1.3 Ⅲ级网络安全事件处置

发生Ⅲ级网络安全事件后，事发单位、行业主管、技术支持单位、公安机关应按照图3所示的Ⅲ级网络安全事件处置流程分别开展工作。

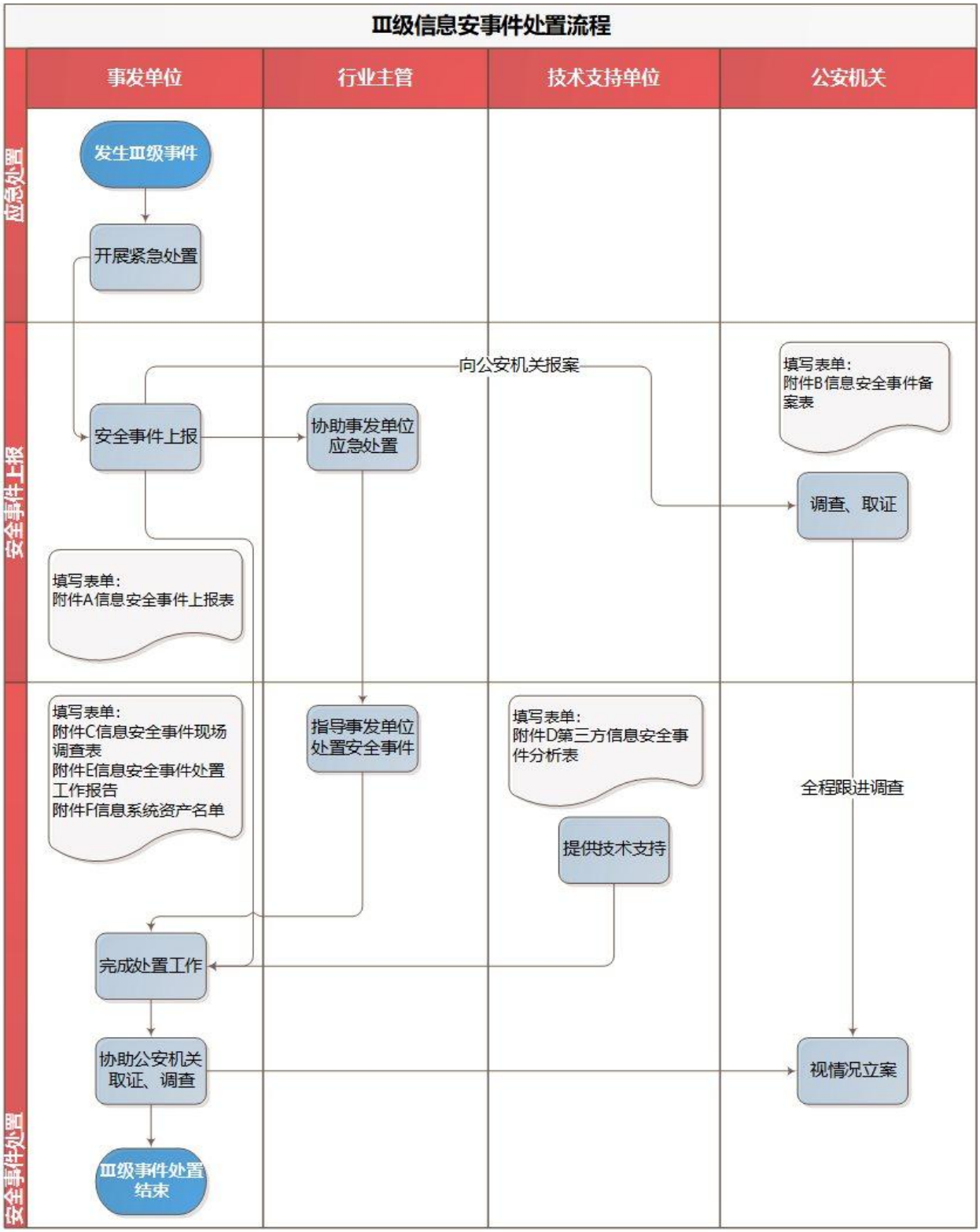

图 3 Ⅲ级网络安全事件处置流程

4.1.1.3.1 网络安全事件处置

发生III级网络安全事件后，开展以下工作：

a) 事发单位应立即开展应急处置工作，并根据情况上报行业主管、协调技术支持单位制定处置方案；
b) 行业主管指导事发单位对安全事件进行处置；
c) 事发单位根据情况向公安机关报案并协助公安机关进行取证、调查工作；
d) 公安机关负责取证、调查以及立案的工作。

4.1.1.3.2 判断网络安全事件类型并进行应急处置

网络安全事件处置小组须及时检查信息系统情况，确认信息安全问题。如果发现该问题涉及范围广且持续造成破坏，应立即断开网络，关闭被破坏系统，保护现场，联系公安机关做进一步处理。

4.1.2 技术措施

网络安全事件处置技术措施包括以下内容，应根据实际情况采取最有效的控制措施加以实施：

a) 备份系统日志、应用日志、数据库日志、审计日志、网络及安全设备日志，用于分析和溯源。同时，检查日志的保存周期，确保日志保存时间 6 个月以上；
b) 保存系统运行状态，包括帐户登录记录、网络连接状态、文件访问状态、进程运行状态等易失数据，以上数据可能包含系统被攻击后的关键信息；
c) 保留被破坏系统的数据、文件、拍照、截图、源代码等，用于分析、溯源及取证；
d) 检测被破坏系统的源代码，分析代码的安全性；
e) 使用专用工具检测操作系统、数据库、应用系统的安全性，发现木马、后门等恶意文件，及时删除；
f) 检测网络设备、安全设备的安全配置情况，包括管理员账号权限与口令、配置策略、日志、访问记录等；
g) 操作系统、应用系统、数据库系统的管理员账号口令重置，检测用户配置策略是否正常；
h) 结束可疑的系统进程，并删除对应的进程文件及目录；
i) 检测应用系统对通过人接口或通信接口输入数据的验证措施是否有效；
j) 操作系统、应用系统、数据库系统的安全补丁更新情况及漏洞扫描检测情况；
k) 对被破坏的 WEB 系统开启 7X24 小时安全检测；
l) 检测异常端口与流量，关闭无关端口，监听异常流量；
m) 备品备件与冗余线路、电路的检查与维护，可随时根据需要替换上线；
n) 门禁系统与视频监控系统的检查，确保功能的可用，用于随时调用和查看；
o) 检测审计系统的工作情况，确保相关审计功能开启、审计内容和记录保存完整；
p) 检测数据通信安全的有效性，确认数据传输经过加密且保证数据完整性；
q) 其他可发现系统隐患或漏洞的技术措施。

4.1.3 证据留存

通过查看被攻击系统的硬件、软件配置参数、审计记录，以及从安全管理制度和人员状况等方面进行取证调查，通过截图、拍照、备份等方式收集被攻击证据，应包含以下方面：

a) 查找信息系统异常现象并对异常现象进行拍照或截图；
b) 留存当前信息系统网络拓扑图；
c) 系统运行状态证据留存；
d) 在保存各文件的同时，保存各文件的哈希校验值；
e) 系统硬件（主机设备、网络设备、安全设备）设备及其配置参数清单；
f) 系统软件（操作系统）、应用软件（数据库、中间件）的配置参数清单；

g) 应用程序文件列表及源代码；
h) 系统运维记录、系统审计日志（网络日志、操作系统日志、数据库日志、中间件日志、应用程序操作日志等）；
i) 网络、操作系统、数据库、中间件、应用程序操作等账号权限（角色、组、用户等）的分配列表；
j) 其他应留存的相关证据。

4.1.4 成因分析

在网络安全事件发生后，应确定被破坏系统的范围。通过对证据的汇总和归纳、现象的推演和还原来论证事件产生的原因，回溯事件发生的过程。网络安全事件成因分析应采取的方法包含以下方面：

a) 了解事件破坏方法、破坏类型、破坏者或恶意程序的标识和特征；对异常文件进行备份；
b) 明确破坏所跨越网络路径，涉及网络区域（外网、内网、子网、骨干网）；
c) 破坏者取得何种权限（破坏是否已取得超级用户特权）；
d) 存的证据进行合理的汇总和归纳。

4.2 事件调查

4.2.1 立案调查

对于网络安全事件造成的影响构成刑事案件，符合立案条件的，应由公安机关案件部门负责对信息安全案件进行案件调查工作。

4.2.2 现场调查

对于网络安全事件造成的影响尚不构成刑事案件，不符合立案条件的，管辖公安机关应按照事件级别开展现场调查工作。要求如下：

a) I 级事件发生后，管辖公安机关信息安全管理部门和案件部门应共同组建事件处置小组，及时前往事发单位对相关事件开展现场调查工作，采取证据提取、人员访谈、笔录制作等方式固定事发系统相关证据，为后续案件侦办或责任调查提供证据；
b) II 级事件发生后，管辖公安机关信息安全管理部门应指派相关工作人员前往事发单位，对现场证据进行固定，为后续案件侦办或责任调查提供证据；
c) III 级事件发生后，管辖公安机关信息安全管理部门应指导事发单位对现场证据进行固定，为后续案件侦办或责任调查提供证据。

4.2.3 责任调查

公安机关对事件的发生原因和各单位存在的责任进行调查。调查的内容包含以下方面：

a) 信息系统异常状态的截图或照片；
b) 事发信息系统的软/硬件设备及其原始数据；
c) 系统运维记录、系统审计日志（网络日志、操作系统日志、数据库日志、中间件日志、应用程序操作日志等）；
d) 发生网络安全事件的系统信息安全等级保护定级和备案工作开展情况；
e) 事发单位对发生网络安全事件的信息系统日常管理情况和安全防护情况；
f) 网络安全事件的责任部门存在的过错或疏忽情况；
g) 其他导致信息系统发生安全事件的情况。

4.2.4 恢复服务和系统加固

网络安全事件的恢复工作应避免出现误操作导致数据的丢失，对于不能彻底恢复配置和清除系统上的恶意文件，或不能肯定系统在根除处理后是否已恢复正常时，应选择彻底重建系统。

系统加固应制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、完善系统备份及冗余措施、增加系统带宽等方法，对系统的安全性进行合理的增强，以达到消除与降低安全风险的目的。此外，在进行系统加固操作前应做好充分的风险规避措施，加固工作应有跟踪记录，以确保系统的可用性。

4.3 事件总结

在网络安全事件得到基本处置后，事发单位应及时对网络安全事件的经过、成因、影响及整改情况进行总结并对其所造成的损失进行评估，填写《网络安全事件处置工作报告》（见附录E），并上报行业主管部门和监管部门；行业主管部门或监管部门应根据事件情况上报市通信保障和信息安全应急指挥部或向相关单位进行通报。对技术难度大、原因不明确的安全事件，专家队伍可进行会商与研判，对网络安全事件进行深入分析，提供解决对策预防此类事件的再次发生。

5 日常防范和应急工作准备

5.1 开展信息安全等级保护工作

信息系统运营使用者及其行业主管部门在日常工作中应切实落实信息系统安全等级保护制度，建立健全安全运维机制，并填报《信息系统资产名单》）（见附录F中表F.1）。

5.2 建立安全运维机制

安全运维机制重点关注信息系统在运行过程中的安全性是否符合信息系统运营使用者及其行业主管部门制定的安全策略和要求。在功能性的运维机制中，加入信息安全要素，如：安全巡检、风险评估、应急策略制定与演练等工作，将安全技术和安全管理统一，形成全面的、无缝的、持续改进的整体。

5.3 开展信息系统安全监测工作

信息系统的服务器及数据库保存大量的重要信息，应定期开展漏洞扫描、渗透测试、安全加固、代码安全审计等工作，以检测结果为基础对安全问题进行汇总分析，形成整改方案并根据优先级逐步实施。对于新系统、新功能的上线，在系统验收时应充分评估安全风险、进行安全检测、做好上线前的突发应急处置措施，确保系统上线后安全运行。

5.4 建立应急响应机制

5.4.1 应急队伍

建立网络与信息安全应急组织，建立网络与信息安全专家库，加强技术交流和技术培训，提高信息系统运营使用者处理突发网络安全事件的能力。

5.4.2 应急物资与装备

根据潜在突发事件的性质和后果，结合信息系统运营使用者情况，制定应急装备与备品备件的配置标准，购置和储备应急所需的物资，制作应急物资清单表。 对应急装备和物资进行定期检查、维护与更新，保证应急物资始终处于完好状态。加强应急备品备件的动态管理，及时补充和更新应急物资清单表。 制定应急物资和装备的年度采购计划，并纳入信息系统运营使用者的年度总预算，切实保证应急物资的资金投入，应急资源清单须每年更新。

5.4.3 通信与信息

应设立网络与信息安全应急 24 小时值班电话，并做到电话号码不变、传真号码不变、电子邮件不变。应急工作相关人员的电话、手机、传真、电子邮件等联系方式应及时更新、及时分发，并保持畅通。

5.4.4 应急响应措施及演练

结合信息系统运营使用者现状建立处置措施、处理流程及演练机制。

为重要信息系统单独制定专项信息安全应急预案，定期演练，确保应急预案的有效性，及时总结演练中发现问题，不断完善应急预案，形成长效的应急处理机制。

对于应急响应工作中发现的安全问题，应持续跟进、反复验证，将详细处置办法及过程结果以应急响应报告的形式进行保存，逐步建立网络安全事件处置知识库。

5.4.5 信息安全意识

信息安全是一项需要长期开展的工作，它不仅涉及技术而且涉及到人员，信息系统运营使用者应关注员工息安全意识，将信息安全意识培训加入年度培训计划，积极宣传信息安全有关的法律法规、安全事件案例分析、内部安全制度等。培训对象不仅包括内部员工还应包括相关第三方用户和服务商。

附 录 A
（规范性附录）
表 A.1 网络安全事件上报表

<table>
<tr><td>信息系统运营使用单位名称</td><td colspan="2"></td><td>报告时间</td><td></td></tr>
<tr><td>报告人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>通讯地址</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td>信息系统名称</td><td colspan="2"></td><td>事发时间</td><td></td></tr>
<tr><td>事件描述</td><td colspan="4"></td></tr>
<tr><td rowspan="9">初步判定的事件类型</td><td rowspan="3">安全攻击</td><td>有害程序</td><td colspan="2">□计算机病毒事件 □蠕虫事件 □特洛伊木马事件 □僵尸网络事件 □混合程序攻击事件 □网页内嵌恶意代码事件 □其他</td></tr>
<tr><td>网络攻击</td><td colspan="2">□拒绝服务攻击事件 □后门攻击事件 □漏洞攻击事件 □网络扫描窃听事件 □网络钓鱼事件 □干扰事件 □其他</td></tr>
<tr><td>信息破坏</td><td colspan="2">□信息篡改事件 □信息假冒事件□信息泄露事件 □信息窃取事件 □信息丢失事件 □其他</td></tr>
<tr><td rowspan="4">设备设施故障</td><td>硬件设备</td><td colspan="2">□服务器 □数据库 □网络设备 □安全设备 □其他</td></tr>
<tr><td>软件设备</td><td colspan="2">□应用系统 □操作系统 □其他</td></tr>
<tr><td>线 路</td><td colspan="2">（说明故障点）</td></tr>
<tr><td>机房基础设施</td><td colspan="2">□盗窃或破坏 □雷击 □失火 □漏水或返潮 □静电 □温湿度 □电力供应 □电磁干扰 □其他</td></tr>
<tr><td rowspan="2">信息安全风险</td><td>可被网络攻击利用</td><td colspan="2">□网络端口被监听 □IP 地址欺骗 □TCP 序号袭击 □病毒 □黑客 □其他</td></tr>
<tr><td>不可被网络攻击利用，但能形成系统故障</td><td colspan="2">□账号管理混乱 □缺乏分级管理□FTP 存在风险 □便携性移动设备控制不严 □其他</td></tr>
<tr><td>造成的影响</td><td colspan="4">□业务中断 □系统破坏 □数据丢失 □其他</td></tr>
</table>

表A.1 网络安全事件上报表（续）

影响范围	□单台主机 □多台主机 □整个信息系统 □整个局域网 □其他
之前是否出现过类似情况	□是（如果是说明发生时间及被破坏系统的名称） □否
初步判定的事件等级	□I 级 □II 级 □III 级
信息系统资产名单	□有 □无
网络安全事件的发展趋势	
预案执行情况	
预案执行结果	
存在问题和改进意见	

附 录 B
（规范性附录）
表 B.1 第三方网络安全事件分析表

<table>
<tr><td rowspan="3">第三方机构</td><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="3">信息系统运营使用单位</td><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2">信息系统名称</td><td colspan="2"></td><td>事发时间</td><td></td></tr>
<tr><td colspan="2">事件描述</td><td colspan="4"></td></tr>
<tr><td rowspan="9">初步判定的事件类型</td><td rowspan="3">安全攻击</td><td>有害程序</td><td colspan="3">☐计算机病毒事件 ☐蠕虫事件 ☐特洛伊木马事件 ☐僵尸网络事件 ☐混合程序攻击事件 ☐网页内嵌恶意代码事件 ☐其他</td></tr>
<tr><td>网络攻击</td><td colspan="3">☐拒绝服务攻击事件 ☐后门攻击事件 ☐漏洞攻击事件 ☐网络扫描窃听事件 ☐网络钓鱼事件 ☐干扰事件 ☐其他</td></tr>
<tr><td>信息破坏</td><td colspan="3">☐信息篡改事件 ☐信息假冒事件☐信息泄露事件 ☐信息窃取事件 ☐信息丢失事件 ☐其他</td></tr>
<tr><td rowspan="3">设备设施故障</td><td>硬件设备</td><td colspan="3">☐服务器 ☐数据库 ☐网络设备 ☐安全设备 ☐其他</td></tr>
<tr><td>软件设备</td><td colspan="3">☐应用系统 ☐操作系统 ☐其他</td></tr>
<tr><td>线 路</td><td colspan="3">（说明故障点）</td></tr>
<tr><td>机房基础设施</td><td colspan="3">☐盗窃或破坏 ☐雷击 ☐失火 ☐漏水或返潮 ☐静电 ☐温湿度 ☐电力供应 ☐电磁干扰 ☐其他</td></tr>
<tr><td rowspan="2">信息安全风险</td><td>可被网络攻击利用</td><td colspan="3">☐网络端口被监听 ☐IP 地址欺骗 ☐TCP 序号袭击 ☐病毒 ☐黑客 ☐其他</td></tr>
<tr><td>不可被网络攻击利用，但能形成系统故障</td><td colspan="3">☐账号管理混乱 ☐缺乏分级管理☐FTP 存在风险 ☐便携性移动设备控制不严 ☐其他</td></tr>
</table>

表 B.1 第三方网络安全事件分析表（续）

之前是否出现过类似情况	□是（如果是说明发生时间及被破坏系统的名称） □否
分析网络安全事件的发展趋势	
初步判定的事件等级	□特别重大事件 □重大事件 □较大事件 □一般事件

附 录 C
（规范性附录）
表 C.1 网络安全事件备案表

<table>
<tr><td rowspan="4">事件发现单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>通信地址</td><td colspan="3">省(自治区、直辖市)_____地(区、市、州、盟)_____县(区、市、旗)</td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="4">信息系统运营使用单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>通信地址</td><td colspan="3">省(自治区、直辖市)_____地(区、市、州、盟)_____县(区、市、旗)</td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="4">受理备案单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>通信地址</td><td colspan="3">省(自治区、直辖市)_____地(区、市、州、盟)_____县(区、市、旗)</td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td>发现时间</td><td colspan="4"></td></tr>
<tr><td rowspan="3">发现途径</td><td>第一类</td><td colspan="3">☐信息系统运营使用单位自行发现</td></tr>
<tr><td>第二类</td><td colspan="3">☐公安机关通过互联网搜索发现
☐公安机关远程漏洞扫描手段发现</td></tr>
<tr><td>第三类</td><td colspan="3">第三方机构通过汇总、分析相关监测数据发现：
☐国家网络与信息安全管理机构 ☐测评机构 ☐信息安全厂商
☐科研院所 ☐其他</td></tr>
</table>

表C.1 网络安全事件备案表（续）

事件类型	安全攻击	有害程序	□计算机病毒事件 □蠕虫事件 □特洛伊木马事件 □僵尸网络事件 □混合程序攻击事件 □网页内嵌恶意代码事件 □其他
		网络攻击	□拒绝服务攻击事件 □后门攻击事件 □漏洞攻击事件 □网络扫描窃听事件 □网络钓鱼事件 □干扰事件 □其他
		信息破坏	□信息篡改事件 □信息假冒事件□信息泄露事件 □信息窃取事件 □信息丢失事件 □其他
	设备设施故障	硬件设备	□服务器 □数据库 □网络设备 □安全设备 □其他
		软件设备	□应用系统 □操作系统 □其他
		线 路	（说明故障点）
		机房基础设施	□盗窃或破坏 □雷击 □失火 □漏水或返潮 □静电 □温湿度 □电力供应 □电磁干扰 □其他
	信息安全风险	可被网络攻击利用	□网络端口被监听 □IP地址欺骗 □TCP序号袭击 □病毒 □黑客 □其他
		不可被网络攻击利用，但能形成系统故障	□账号管理混乱 □缺乏分级管理□FTP存在风险 □便携性移动设备控制不严 □其他
之前是否出现过类似情况		□是_____（发生时间及被破坏系统的名称） □否	

附 录 D
（规范性附录）
表 D.1 网络安全事件现场调查表

<table>
<tr><td rowspan="3">受理备案单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="3">应急处置队伍</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="3">信息安全专家组</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="3">行业主管部门</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系人</td><td></td></tr>
<tr><td>传真</td><td></td><td>传真</td><td></td></tr>
<tr><td rowspan="3">信息系统运营使用单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="5">被破坏信息系统现状</td><td>信息系统名称</td><td colspan="3"></td></tr>
<tr><td>造成的影响</td><td colspan="3">□业务中断 □系统破坏 □数据丢失
□其他</td></tr>
<tr><td>影响范围</td><td colspan="3">□单台主机 □多台主机 □整个信息系统 □整个局域网 □其他</td></tr>
<tr><td>信息系统资产名单</td><td colspan="3">□当前系统结构拓扑图 □系统硬件设备及其配置参数清单 □系统软件、应用软件的配置参数清单 □应用程序文件列表及源代码 □系统运维记录 □系统审计日志 □账号权限分配列表 □单位应急处置人员联系表 □其他</td></tr>
<tr><td>预处理措施</td><td colspan="3"></td></tr>
</table>

表D.1 网络安全事件现场调查表（续）

<table>
<tr><td rowspan="12">事件处置</td><td colspan="2">分析事件成因</td><td colspan="2"></td></tr>
<tr><td rowspan="11">判定事件类型</td><td rowspan="3">安全攻击</td><td>有害程序</td><td>□计算机病毒事件 □蠕虫事件 □特洛伊木马事件 □僵尸网络事件 □混合程序攻击事件 □网页内嵌恶意代码事件 □其他</td></tr>
<tr><td>网络攻击</td><td>□拒绝服务攻击事件 □后门攻击事件 □漏洞攻击事件 □网络扫描窃听事件 □网络钓鱼事件 □干扰事件 □其他</td></tr>
<tr><td>信息破坏</td><td>□信息篡改事件 □信息假冒事件□信息泄露事件 □信息窃取事件 □信息丢失事件 □其他</td></tr>
<tr><td rowspan="4">设备设施故障</td><td>硬件设备</td><td>□服务器 □数据库 □网络设备 □安全设备 □其他</td></tr>
<tr><td>软件设备</td><td>□应用系统 □操作系统 □其他</td></tr>
<tr><td>线 路</td><td>（说明故障点）</td></tr>
<tr><td>机房基础设施</td><td>□盗窃或破坏 □雷击 □失火 □漏水或返潮 □静电 □温湿度 □电力供应 □电磁干扰 □其他</td></tr>
<tr><td rowspan="2">信息安全风险</td><td>可被网络攻击利用</td><td>□网络端口被监听 □IP 地址欺骗 □TCP 序号袭击 □病毒 □黑客 □其他</td></tr>
<tr><td>不可被网络攻击利用，但能形成系统故障</td><td>□账号管理混乱 □缺乏分级管理□FTP 存在风险 □便携性移动设备控制不严 □其他</td></tr>
<tr><td colspan="2">判定事件级别</td><td colspan="2">□一级 □二级 □三级</td></tr>
<tr><td colspan="2">保留证据</td><td colspan="2">□被攻击操作系统信息 □日志信息
□帐号信息 □源代码信息
□其他</td></tr>
</table>

表D.1 网络安全事件现场调查表（续）

事件处置	勘察现场	□最新的信息系统网络拓扑图 □系统硬件设备及其配置参数清单（□主机设备 □网络设备 □安全设备 □其他_____） □系统软件的配置参数清单（□操作系统 □数据库 □中间件 □其他_____） □应用程序文件列表及源代码 □系统运维记录 □系统审计日志（□网络日志 □操作系统日志 □数据库日志 □中间件日志 □应用程序操作日志 □其他_____） □账号权限（角色、组、用户等）分配列表（□网络 □操作系统 □数据库 □中间件 □应用程序 □其他_____）
	消除影响的措施	
	溯源攻击的过程及结果	
	系统恢复的过程及结果	
	后期整改建议	
处置人员签字	现场民警	
	应急处置队伍代表	
	信息安全专家组代表	
	行业主管部门负责人	
	事发单位负责人	

附 录 E
（规范性附录）
网络安全事件处置工作报告

E.1 事件经过

简述该网络安全事件的发现、处理及上报经过。

E.2 事件成因

描述该网络安全事件发生的起因。如：由自然灾害、故障（电力中断故障、网络损坏或是软件故障、硬件设备故障等）、人为破坏（破坏网络线路、破坏通信设施，黑客攻击、病毒攻击、恐怖袭击）等引起的安全事件。

E.3 评估事件影响

描述网络安全事件发生后，造成的影响和影响范围。如：多个应用系统业务中断，造成多台服务器宕机，重要业务数据丢失等。

E.4 整改措施

描述信息系统运营使用单位发生安全事件后，处理的措施和处理结果。如：保留证据、查看配置、消除影响、溯源攻击、恢复服务及后期整改等。

E.5 其他情况

事发系统定级、备案、测评等情况

附 录 F
（规范性附录）
表 F.1 信息系统资产名单

信息系统名称			
承载业务情况	业务描述		
	用户分布范围	□全国 □全省 □本地区 □本单位	
系统结构拓扑图	□有 □无 □不适用		
系统硬件设备	主机设备	台数	
		其配置参数清单	□有 □无 □不适用
	网络设备	台数	
		其配置参数清单	□有 □无 □不适用
	安全设备	台数	
		其配置参数清单	□有 □无 □不适用
系统软件	系统软件	操作系统	
		其配置参数清单	□有 □无 □不适用
	应用软件	数据库	
		其配置参数清单	□有 □无 □不适用
		中间件	
		其配置参数清单	□有 □无 □不适用
应用程序	文件列表	□有 □无 □不适用	
	源代码	□有 □无 □不适用	
系统运维记录	□有 □无 □不适用		
系统审计日志	网络日志	□有 □无 □不适用	
	操作系统日志	□有 □无 □不适用	
	数据库日志	□有 □无 □不适用	
	中间件日志	□有 □无 □不适用	
	应用程序操作日志	□有 □无 □不适用	

表F.1 信息系统资产名单（续）

账号权限分配列表	网络账号	□有 □无 □不适用
	操作系统账号	□有 □无 □不适用
	数据库账号	□有 □无 □不适用
	中间件账号	□有 □无 □不适用
	应用程序操作账号	□有 □无 □不适用
单位应急处置人员联系表	□有 □无 □不适用	

参 考 文 献

[1]北京市社会领域网络与网络安全事件应急预案
[2]北京市公安局网络安全保卫总队关于印发网络与信息系统安全事件应急处置流程的通知